SOPHOS

Security made simple.

Sophos Mobile Control
Startup guide

Product version: 5.1
Document date: July 2015

Contents

1 About this guide

This guide tells you how to initially configure Sophos Mobile Control step by step to manage your mobile devices.

Further information is available in the *Sophos Mobile Control administrator guide*.

This guide focuses on iOS and Android as the most common mobile platforms. The settings apply to other operating systems in a similar way.

1.1 Terminology

In this guide, the following terms are used:

Term	Explanation
Device	The mobile device to be managed (for example smartphone or tablet).
Sophos Mobile Control client	The Sophos Mobile Control client component that is installed on the device.
End user	The end user of the device.
Web console	The web interface of the server that is used to manage devices.
Customer	The tenant that manages devices.
Enrollment	The process of equipping devices with the Sophos Mobile Control client. **Note:** This process is also called provisioning.
Task bundle	A package you can create in the web console to bundle several tasks for mobile devices in one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.
Self Service Portal (SSP)	The Sophos Mobile Control web interface that allows end users to enroll their own devices and carry out other tasks without having to contact the helpdesk.
Sophos Mobile Security	A security app for Android phones and tablets. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.

Term	Explanation
SMSec	Abbreviation for Sophos Mobile Security used in the Sophos Mobile Control web console user interface.
Sophos Secure Workspace	An encryption app for iOS and Android phones and tablets. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.

2 Sophos Mobile Control licenses

Sophos Mobile Control offers two types of license:

- Standard license
- SMC Advanced license

  An SMC Advanced license adds functionality by enabling you to manage **Sophos Mobile Security** and **Sophos Secure Workspace**.

  - Sophos Mobile Security is a security app for Android phones and tablets that protects devices from malicious apps and assists end users in detecting app permissions that could be a security risk.
  - Sophos Secure Workspace is an app for iOS and Android phones and tablets that allows users to access encrypted files stored in the cloud. Files can be decrypted and viewed in a seamless way. Encrypted files can be handed over by other apps and uploaded to one of the supported cloud storage providers. Alternatively the documents can be stored locally within the app.

    With Sophos Secure Workspace you can read files encrypted by SafeGuard Cloud Storage or SafeGuard Data Exchange. Both are modules of SafeGuard Enterprise or one of its different editions. They allow you to encrypt files using a local key. These local keys are derived from a passphrase that is entered by a user. You can only decrypt a file when you know the passphrase that was used to encrypt the file.

    For details of the SafeGuard Cloud Storage and SafeGuard Data Exchange modules please refer to the SafeGuard Enterprise 7.0 documentation on www.sophos.com.

2.1 Trial licenses

Sophos offers a free trial for Sophos Mobile Control. You can register for the trial on the Sophos website: http://www.sophos.com/en-us/products/free-trials/mobile-control.aspx.

A trial license allows you to manage up to five users and is valid for 30 days.

All you will need when you set up Sophos Mobile Control for evaluation is the email address you used to register when downloading the installer.

3 What are the key steps?

To start using Sophos Mobile Control:

1. Log in to the Sophos Mobile Control web console as a super administrator.
2. Carry out the initial configuration of the Sophos Mobile Control server.

   Note: If necessary, the configuration wizard is launched automatically when you log in as a super administrator. If initial configuration has already been done, for example after installation, go directly to step 3.

   If you activate your Standard and Advanced licenses in this step, go directly to step 4.

3. Check your licenses.
4. Create a new customer for managing your devices.
5. Switch to the new customer.
6. Create an administrator for the new customer and log in at the web console as that administrator.
7. Configure personal settings, password policies for web console users and technical contact, settings for the Self Service Portal.
8. Create and upload an Apple Push Notification service certificate.
9. Configure compliance rules.
10. Create device groups.
11. Configure devices.
12. Update Self Service Portal settings, add a Self Service Portal user and test Self Service Portal enrollment.
13. Add users either by creating them or by uploading your user list.

4 Log in as a super administrator

Prerequisite:

- A super administrator account has been created during Sophos Mobile Control setup and you have the credentials (customer, user name and password) for the account.

Before you can start to configure Sophos Mobile Control, you have to log in to the Sophos Mobile Control web console as a super administrator. The super administrator customer offers a specific view of the Sophos Mobile Control web console that is customized for super administrator tasks.

Note: For a detailed description of how to use the Sophos Mobile Control web console as a super administrator, refer to the *Sophos Mobile Control super administrator guide*.

1. Enter the Sophos Mobile Control web console URL in your preferred web browser.

   The Sophos Mobile Control login page is displayed.

2. In the **Customer** field, enter the super administrator customer.
3. In the **User** and **Password** fields, enter your super administrator user name and password.
4. Click **Login**.

You are logged in to the super administrator customer. Depending on whether initial configuration has already been done or not:

- The configuration wizard is launched.
- The super administrator customer **Dashboard** is displayed. The current customer is displayed in the upper-right corner of the Sophos Mobile Control web console. The super administrator customer is marked by an asterisk and shown at the top of the drop-down list.

5 Initial configuration of the Sophos Mobile Control Server

Before you can use the Sophos Mobile Control web console you need to configure certain server settings. Sophos Mobile Control provides a configuration wizard to guide you through this.

The wizard is launched automatically when you log in to the Sophos Mobile Control web console for the first time after installation.

You need to provide:

- HTTP proxy credentials (optional)
- A Standard license key and/or an Advanced license key
- SSL certificate(s)
- SMTP credentials

Note: You can request a trial license when the configuration wizard is run.

5.1 Configuration wizard

Note: As a super administrator you can change these settings in the Sophos Mobile Control web console at any time after initial configuration.

1. After you have logged in to the Sophos Mobile Control web console the **Welcome** view is displayed. Click **Next**.
2. If you use a HTTP proxy, enter the relevant server details in the **HTTP proxy** view:
   a) Select **Proxy enabled**.
   b) Enter the **Proxy host**.
   c) Enter the **Proxy port**.
   d) Click **Next**.

3. In the **License** view, enter your Sophos Mobile Control Standard license key or request a trial license:

   - **Sophos Mobile Control Standard license key:**

     When you enter the Sophos Mobile Control Standard license key and click **Activate**, you are given the option to enter a Sophos Mobile Control Advanced license key. If you have purchased Advanced licenses, enter the key in the **Advanced license key** field.

   - **Request a trial license:**

     If you are evaluating Sophos Mobile Control, see Trial licenses (page 6), click **Request trial** and enter the email address that you used during the registration process of your free trial, and then click **Request trial** again.

   Note: You can change the license settings at any time in the Sophos Mobile Control web console. If you do not enter an **Advanced license key** here, you can do it in the web console later on.

   Click **Next**.

4. In the **SSL** view, enter the certificates to be used for securing the SSL connection between server and clients. The certificates guarantee the authenticity of the server. The clients will only trust the certificates specified here (certificate pinning).

   a) Click the **Auto-discover certificate(s)** button.

      In most cases the auto-discover function is sufficient to discover the certificates currently in use.

   b) If the certificates cannot be discovered automatically, you can upload them by clicking **Upload a file**, selecting the desired file (.CER or .DER) and clicking **Open**.

   The certificates are displayed in the **SSL** view. Sophos Mobile Control supports up to four certificates. If a certificate is no longer valid the client will use any other valid certificate from the list to establish the SSL connection to the server.

   Note: You have to update the list after changing or renewing SSL certificates. It is important to ensure that at least one valid certificate is always available. Otherwise the clients will not trust the server and will no longer connect to it, until the list has been updated.

5. SMTP has to be configured to enable emails to be sent to new users, providing them with logon credentials. It also needs to be configured to enable enrollment via email. In the **SMTP** view, enter SMTP information and logon credentials:

   - **SMTP host**
   - **Connection Type** (SSL, TSL or plain)
   - **SMTP user**
   - **SMTP password**
   - **Email originator**
   - **Send error emails**: Select this option if you want error mails to be sent, for example in case of an expired APNs certificate.
   - **Email recipients**: Enter the recipients of error emails here.

   Note: To check sending of emails, click the **Send test email** button.

6. Click **Finish**

6 Check your licenses

Note: For Sophos Mobile Control a user-based license scheme applies. One user license is valid for all devices assigned to that user. Devices that are not assigned to a user require one license each.

In the web console, under **SYSTEM**, click **System setup**, go to the **License** tab and check the license information:

- **Number of licenses:**

  Shows the number of end users that can be managed from the web console.

- **Licenses used:**

  Shows the number of licenses in use.

- **Valid until:**

  Shows the license expiry date.

If you have any questions or concerns regarding the license information shown, contact your Sophos Sales representative.

6.1 Activate Sophos Mobile Control Advanced licenses

Sophos Mobile Security and Sophos Secure Workspace management are optional modules of Sophos Mobile Control. If the Advanced license was not activated during initial configuration, you can activate it in the Sophos Mobile Control web console now:

1. In the web console, under **SYSTEM**, click **Setup** and then **System setup**.

   The **System setup** view is displayed.

2. On the **License** tab, enter the **Advanced license key** you have received from Sophos in the appropriate field and click **Activate**.
   - The **Active license key** field shows the activated license key.
   - The **Number of licenses** field shows the number of end users that can be managed from the web console.
   - The **Valid until** field shows the license expiry date.

When you create a new customer, you can assign the number of end users you want to manage for this customer. You can enable management functionality for Sophos Mobile Security and Sophos Secure Workspace for each customer separately.

7 Create customers

1. In the super administrator customer **Dashboard**, click the **Create customer** button.
2. The **Edit customer** view is displayed.
3. Enter a **Name** and a **Description** for the new customer.
4. In the **Maximum number of licenses** field, define how many users can be managed for this customer.
5. If you have activated an SMC Advanced license, the **Advanced licenses** checkbox is displayed. Select **Advanced licenses**, if you want the customer to be capable of managing Sophos Mobile Security and Sophos Secure Workspace. For further information, see the *Sophos Mobile Control administrator guide*.
6. In the **Valid until** field, specify the expiry date for the customer. If you do not specify an expiry date here, **unlimited** is shown in the **Valid until** column in the customer overview.
7. Under **Activated platforms**, select the platforms for which devices may be registered for the customer.
8. Under **Locate devices**, select **Allowed for users** to enable users to locate their devices if they are lost or stolen. Select **Allowed for administrators** to enable administrators to locate devices.
9. Under **Clone Settings**, select the **Settings and packages** checkbox if you want all profiles, bundles, and packages created in the super administrator account to be available in the customer's account. For more information about cloning, see the *Sophos Mobile Control super administrator guide*.
10. Under **User directory**, select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile Control:
    - **None. No SSP and user-specific profiles available.**
    - Select **Internal directory** to use internal user management for users of the Sophos Mobile Control Self Service Portal. For further information, see the *Sophos Mobile Control administrator guide*.
    - Select **External LDAP directory** to use external user management for users of the Sophos Mobile Control Self Service Portal. Click **Configure external LDAP** to specify the server details. For further information, see the *Sophos Mobile Control super administrator guide*.
11. Click the **Save** button.

The customer is created and displayed on the **Dashboard**.

8 Switch to the new customer

Switch to the new customer to carry out further required steps:

1. In the super administrator customer **Dashboard**, the current customer is displayed in the upper-right corner. The super administrator customer is marked by an asterisk and shown at the top of the drop-down list.
2. Select the customer you have created from the drop-down list.

The Sophos Mobile Control web console changes from the specific super administrator view to the regular view. You can now carry out further required steps for initial configuration.

9 Create an administrator for the new customer

1. In the web console, under **SYSTEM**, click **Setup** and then click **Administrators**.

   The **Show administrators** view is displayed.

2. Click the **Create administrator** button.

   The **Edit administrator** view is displayed.

3. Enter a **Login name** for the new user.
4. From the **Role** dropdown list, select the user role **Administrator**.
5. Enter the **First name** and the **Last name** of the new user.
6. Enter the **Email address** of the new user.
7. Enter a one-time **Password** for the first login at the web console and confirm it.
8. Click the **Save** button.

The new administrator is created. To carry on with the next steps, you need to log out from the web console and log in with the new credentials (user, customer and one-time password) again. You will be prompted to change the password at first login.

10 Configure settings

The following settings need to be configured:

- Personal settings, for example the platforms you want to manage
- Password policies
- Technical contact
- Settings for the use of the Self Service Portal by end users

10.1 Configure personal settings

To use the Sophos Mobile Control web console more efficiently, you can customize the user interface to show only the platforms you work with.

Note: By configuring the platforms you only change the view of the user who is currently logged on. You cannot deactivate any functions here.

Prerequisite: You have logged in at the web console as the administrator you have created for the new customer.

1. In the web console, under **SYSTEM**, click **Setup** and then **General**.

   The **General settings** view is displayed.

2. Go to the **Personal** tab.
3. Configure the following settings:

   a) In the **Language** field , select the language for the Sophos Mobile Control web console.

   b) In the **Timezone** field, select the timezone.

   c) In the **Lines per page in tables** field, select the maximum number of table lines you want to display per page in the web console. You can choose between **20** and **100** lines.

   d) Select **Show Extended device details** to show all available information of the device. The tabs **Custom properties** and **Internal properties** will be added to the **Show device** view.

   e) Under **Activated platforms**, select the platforms you want to use in the web console: **Android**, **iOS** and **Windows Phone** are supported. If you select specific platforms, you can only use the selected platforms with Sophos Mobile Control. All other platforms are hidden. In addition, all modules and functions that are not required for a specific platform are hidden.

   Note: The list of available platforms depends on your platform settings from the super administrator configuration. For further information, see the *Sophos Mobile Control super administrator guide*.

   Note: This guide focuses on iOS and Android. For further information on all available platforms, see the *Sophos Mobile Control administrator guide*.

   The menu is customized according to your settings. Unnecessary items are hidden.

4. Click the **Save** button.

10.2 Configure password policies

To enforce password security, configure password policies for users of the Sophos Mobile Control web console and the Self Service Portal.

Note: If you use internal user management, the password policies apply to web console users and Self Service Portal users. If you use external user management, these password policies only apply to web console users. In this guide, internal Self Service Portal user management is described as an example. For further information on external user management, see the *Sophos Mobile Control super administrator guide*.

1. In the web console, under **SYSTEM**, click **Setup** and then **General**.

   The **General settings** view is displayed.

2. Go to the **Password policies** tab.
3. Under **Password policies for SMC web console user** - **Rules**, define the required minimum values for the password.
4. Under **Password policies for SMC web console user** - **Settings**, define the following settings:
   - **Password change interval (days)**: You can enter a value from **0** (no password change required) to **730** days.
   - **Number of previous passwords which must not be reused**: You can select a value between **1** and **10**.
   - **Maximum number of failed login attempts**: You can select a value between **1** and **10**.
5. Click the **Save** button.

10.3 Configure technical contact

To support users who have questions or problems, you can configure technical contact information. The information you enter here will be displayed in the Sophos Mobile Control app and in the Self Service Portal.

1. In the web console, under **SYSTEM**, click **Setup** and then **General**.

   The **General settings** view is displayed.

2. Go to the **Technical contact** tab.
3. Enter the required information for the technical contact. Under **Additional information**, you can enter information for supporting users who have questions or problems.
4. Click the **Save** button.

10.4 Configure Self Service Portal settings

1. In the web console, under **SYSTEM**, click **Setup** and then click **Self Service Portal**.

   The **Self Service Portal** view is displayed.

2. On the **Configuration** tab, configure the Self Service Portal settings as required. For further information on all available settings, see the *Sophos Mobile Control administrator guide*. If you are not sure which settings to apply at this stage, you can also leave all options at their default settings.
3. Go to the **Agreement** tab.
4. Configure a mobile policy disclaimer or agreement text that is displayed as a first step when end users register their devices. Users have to confirm that they have read this text to be able to continue.

   Simple HTML formatting tags are supported for the text. The text will be displayed in the relevant browser accordingly.
5. Go to the **Post-install text** tab (optional).
6. Configure text to be displayed after the automatic installation steps in the Self Service Portal. This text can give the user guidance for the next required steps.

   Simple HTML formatting tags are supported for the text. The text will be displayed in the relevant browser accordingly.
7. Click the **Save** button.

11 Create and upload an APNs certificate

To use the built-in Mobile Device Management (MDM) protocol of devices running Apple iOS 4 (or higher), Sophos Mobile Control must use the Apple Push Notification service (APNs) to trigger iOS devices.

Prerequisites:

- You have configured the iOS platform for this customer, see Configure personal settings (page 16).
- You can use the APNs Certificate Wizard to create an APNs certificate. The wizard is included in your product delivery. It is also available for download in the web console. In the web console menu bar, under **SYSTEM**, click **Setup** and then **System setup**,and go to the **iOS APNS** tab. To download the wizard, click the download link available under **APNS**.

To start the APNs Certificate Wizard:

1. Double-click the file Sophos Mobile Control APNs Certificate Wizard.exe.

   The APNs Certificate Wizard welcome dialog is displayed.

2. Click **Next**.

   The **License Agreement** dialog is displayed.

3. Click **I agree**.

   The **Create Certificate Signing Request** dialog is displayed.

4. Enter your **Company Name** and your **Country** code (for example US or UK). These fields are mandatory.

   Note: Below these fields, the dialog shows where all data of the process is stored. Make a note of this information.

5. Click **Next**.

   The **Upload PLIST** dialog is displayed.

6. In this step, you upload the Certificate Signing Request to Apple. Follow the instructions in the dialog:

   a) Open the Apple site indicated in the dialog in your browser.

      Note: Do not use Internet Explorer to open the Apple site as this may cause problems. Use Firefox, Chrome or Safari instead. We recommend that you use the latest browser versions.

   b) Log in with your Apple ID. If you do not have an Apple ID, create one.

We recommend you create a Corporate Apple ID and not a personal one.

c) In the first dialog of the **Apple Push Certificates Portal**, click **Create a Certificate**.

d) Accept the terms and conditions.

e) Browse for your Certificate Signing Request (*.plist) and click **Upload**.

You find the file name and the path in the **Upload PLIST** dialog of the Sophos APNs Certificate Wizard.

Your APNs certificate is created.

f) Download and save the certificate file (*.pem) in the directory indicated in the **Upload PLIST** dialog.

7. Click **Next**.

The **Create P12** dialog is displayed.

8. In this step, you create your APNs certificate for Sophos Mobile Control. Enter a password for the APNs certificate. You need this password later, when you upload the .P12 certificate file to Sophos Mobile Control.

Note: The **Create P12** dialog shows the directory the certificate will be stored in. Make a note of this information. We recommend that you create a backup of the folder that contains the certificate files.

9. Click **Next**.

The **Sophos Mobile Control APNs Certificate Wizard finished** dialog is displayed.

10. Click **Finish**.
11. In the web console return to the **iOS APNs** tab.
12. Click on **Upload a file**. Browse for the .p12 certificate file you have created and enter your password. Optionally you can enter your Apple ID for future reference.

After the file has been uploaded successfully, a confirmation message is displayed and the **Topic**, **Type** and **Expiry date** information of your APNs certificate is shown.

13. Click **Save**.

12 Configure compliance rules

In the web console, you can:

- Configure compliance rules for all available device types (platforms).
- Define actions to be taken if devices no longer comply with the rules specified.
- Define multiple compliance rules and assign them to device groups. In device groups, you can select different compliance rules for company or employee devices. This allows you to apply different levels of security to different **Device groups**.

For further information, see the *Sophos Mobile Control administrator guide*.

1. In the web console, under **CONFIGURE**, click **Compliance rules**.

   The **Compliance rules** list view is displayed.

2. Click the **Create compliance rules** button.

   The **Compliance rules** view with tabs for all available device platforms is shown.

3. Enter a **Name** and a **Description** for the new compliance set.
4. Go to the required device platform tab.
5. Make sure that the **Enable platform** checkbox is selected.

   Note: If this checkbox is not selected, devices of the relevant platform will not be checked for compliance.

6. Under **Rule**, configure the compliance requirements for the selected device type. For a description of all settings available for each device type, see the *Sophos Mobile Control administrator guide*.
7. To disallow email access if particular rules are not met, select the checkbox **Deny ActiveSync** next to the corresponding rules.

   Note: This setting only becomes effective if you use the Sophos Mobile Control EAS Proxy server. For further information, see the *Sophos Mobile Control installation guide*.

8. To disallow document access if particular rules are not met, select the checkbox **Deny document access** next to the corresponding rules.

   Note: Denying document access is only possible if you are using an SMC Advanced license.

9. To disallow network access if particular rules are not met, select the checkbox **Deny network access** next to the corresponding rules.

   Note: This setting is only available if the network access control functionality has been activated. For further information, see the *Sophos Mobile Control super administrator guide*.

10. To notify administrators if particular rules are not met, select the checkbox **Notify admin** next to the corresponding rules.

    Note: You have to enter the recipients' email addresses and the schedule for sending emails under **Compliance email settings**. See step 13.

11. Under **Transfer task bundle**, you can select task bundles to be transferred for the required **Rule** settings. Leave the fields unchanged at this stage. When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required. For further information, see the *Sophos Mobile Control administrator guide*.
12. After you have defined all settings in all required device type tabs, click the **Save** button.

    The new compliance rule is displayed in the **Compliance rules** list view.

13. If you have set administrators to receive email notifications when devices are not compliant, specify the relevant recipients under **Compliance email recipients** and a notification schedule under **Compliance email schedule**. Use semicolons (**;**) to separate several administrators in the **Compliance email recipients** field. Click the **Save** button.

To add further compliance rules, repeat the described steps. You can assign the created compliance rules when you create a device group in the next step. If you plan to manage corporate and private devices, we recommend that you define separate rules for at least these two device types.

13 Create device groups

We recommend that you put devices into groups. This helps you to manage them efficiently as you can carry out tasks on a group rather than on individual devices.

Note: We recommend that you only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

To create a new device group:

1. In the web console, under **MANAGE**, click **Device groups**.

   The **Device groups** view is displayed.

2. Click the **Create device group** button.

   The **Edit device group** view is displayed.

3. Enter a **Name** and a **Description** for the new device group.
4. Under **Compliance rules** in the fields **Company devices** and **Employee devices**, select the compliance rules you want to apply.
5. Click the **Save** button.

   Note: The device group settings contain the **Enable auto-enrollment** option. This option allows you to enroll iOS devices with the Apple Configurator. For further information, see the *Sophos Mobile Control administrator guide*.

The new device group is created and shown in the **Device groups** view. You can now add devices to the new group.

Note: If you delete a device group, the group's members are moved to another group that needs to be specified. If there is no other group left to move the devices to, the group cannot be deleted. Before a group is deleted a warning message is displayed.

14 Configure iOS devices

14.1 Create profiles for Apple iOS devices

In this step, you create a profile for initial configuration of iOS devices. A recommended initial configuration should include your password policies and the restrictions you want to apply to devices. We recommend that you include Exchange, VPN and Wi-Fi settings in separate profiles.

Note: Sophos Mobile Control offers two methods for creating profiles for iOS devices:

- You can create iOS profiles directly in the web console.
- You can import profiles created with Apple Configurator into the web console.

This section describes how to create profiles directly in the web console. For further information on how to import profiles created with Apple Configurator, see the *Sophos Mobile Control administrator guide*.

1. In the web console, under **CONFIGURE**, click **Profiles** and then **Apple iOS**.

   The **Profiles** view is displayed.

2. Click the **Create profile** button and select **Create profile**.

   The **Edit profile** view is displayed.

3. Enter a **Name** for the new profile.

   We recommend that you use the name "iOS SSP profile" for profiles that are applied during the enrollment process through the Self Service Portal.

4. In the **Organization** field, enter the name of the organization for the profile, for example a company name.
5. Enter a **Version** for the new profile.
6. In the **Description** field, enter a description for the profile, for example "base profile".
7. In the **User can remove profile** drop-down list, select whether users may remove the profile from their device:

   - **Always**
   - **With authentication**
   - **Never**

   Note: We recommend that you select the option **Never**.

8. In the **Automatically remove on** field, you can select a date for the automatic removal of the profile from end user devices.

   Note: We recommend that you do not configure a date for the automatic removal of the profile.

   Note: This function is supported as of iOS 6.

9. Under **Operating systems**, select the operating system the profile should apply to. Select all iOS versions for this profile.

   Note: The operating system list is created according to devices registered with the system. At this stage, it may show only **iOS**. The setting **iOS** covers all iOS versions.

10. Click the **Add configuration** button to add configurations with iOS settings to the profile.

    The **Available configurations** view is displayed.

11. Select **Password policies** and click **Next**.

    The **Password policies** view is displayed.

12. Specify the password policies settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
13. Click the **Apply** button.

    The **Password policies** configuration is displayed in the **Edit profile** view under **Configurations**.

14. To add **Restrictions** settings, click the **Add configuration** button again.

    Note: Supported settings may depend on the iOS version in use on individual devices. Depending on the end user device, some settings may not have any effect. If settings require a certain iOS version, it is displayed next to the option. For further information, see the feature matrix in the *Sophos Mobile Control technical guide*.

15. In the **Available configurations** view, select **Restrictions** and click **Next**.

    The **Restrictions** view is displayed.

16. Specify the restrictions settings for this profile. For a detailed description of all settings available, see the *Sophos Mobile Control administrator guide*.
17. Click the **Apply** button.

    The **Restrictions** configuration is displayed in the **Edit profile** view under **Configurations**.

18. Click the **Save** button.

The profile is available for transfer. It is displayed in the **Profiles** view. To configure profiles with Exchange, VPN and Wi-Fi settings, repeat the steps described.

14.2 Create task bundles for iOS devices

1. In the web console, under **CONFIGURE**, click **Task bundles** and then click **Apple iOS**.

   The **Task bundles** view is displayed.

2. Click the **Create task bundle** button.

   The **Edit task bundle** view is displayed.

3. Enter a **Name** and a **Version** for the new task bundle.

   We recommend that you use the name "iOS SSP task bundle" for task bundles that are applied during the enrollment process through the Self Service Portal.

4. In the **Description** field, enter a description for the bundle, for example "base SSP task bundle".
5. Under **Operating systems**, select the operating systems the task bundle applies to. Select all iOS versions for this task bundle.

   Note: The operating system list is created according to devices registered with the system. At this stage, it may show only **iOS**. The setting **iOS** covers all supported iOS versions.

6. Under **Tasks**, click the **Create task** button.
7. As a first task, select **Enroll**. Enter a task name and click **Apply**. The name you define here is shown in the Self Service Portal while tasks are processed.
8. Create a second task of the type **Install profile**. Give the task a meaningful name, for example "Install provisioning profile", select the profile you have created ("iOS SSP profile", if you have used the suggested name) and click **Apply**. If you have configured profiles with Exchange, VPN and Wi-Fi settings, repeat this step for each profile.
9. Repeat this procedure to add further tasks. You can set the order for installation for selected tasks by using the sort arrows on the right-hand side of the **Tasks** list.
10. After you have added all required tasks to the task bundle, click the **Save** button in the **Edit task bundle** view.

The task bundle is available for transfer. It is displayed in the **Task bundles** view.

15 Configure Android devices

15.1 Create profiles for Android devices

In this step, you create a profile for initial configuration of Android devices. A recommended initial configuration should include your password policies and the restrictions you want to apply to devices. We recommend that you include Exchange, VPN and Wi-Fi settings (if your Android devices support these settings) and upload root and client certificates in separate profiles.

1. In the web console, under **CONFIGURE**, click **Profiles** and then click **Android**.

   The **Profiles** view is displayed.

2. Click the **Create profile** button and select **Create device profile**.

   The **Edit profile** view is displayed.

3. Enter a **Name** and a **Version** for the new profile.

   We recommend that you use the name "Android SSP profile" for profiles that are applied during the enrollment process through the Self Service Portal.

4. In the **Description** field, enter a description for the profile, for example "base profile".
5. Under **Operating systems**, select the operating system the profile should apply to. Select all Android versions for this profile.

   Note: The operating system list is created according to devices registered with the system. At this stage, it may show only **Android**. The setting **Android** covers all supported Android versions.

6. Click the **Add configuration** button to add configurations with Android configuration settings to the profile.

   The **Available configurations** view is displayed.

7. Select **Password policies** and click **Next**.

   The **Password policies** view is displayed.

8. In the **Password type** field, select the type of password you want to define, for example **Complex**.
9. Specify the password policies settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
10. Click the **Apply** button.

    The **Password policies** configuration is displayed in the **Edit profile** view under **Configurations**.

11. To add **Restrictions** settings, click the **Add configuration** button again.

    Note: Supported settings may depend on the Android version in use on individual devices. Depending on the end user device, some settings may not have any effect. If settings require a certain Android version, it is displayed next to the option. For further information, see the feature matrix in the *Sophos Mobile Control technical guide*.

12. In the **Available configurations** view, select **Restrictions** and click **Next**.

    The **Restrictions** view is displayed.

13. Specify the restrictions settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
14. Click the **Apply** button.

    The **Restrictions** configuration is displayed in the **Edit profile** view under **Configurations**.

15. Click the **Save** button.

The profile is available for transfer. It is displayed in the **Profiles** view.

15.2 Create task bundles for Android devices

1. In the web console, under **CONFIGURE**, click **Task bundles** and then click **Android**.

   The **Task bundles** view is displayed.

2. Click the **Create task bundle** button.

   The **Edit task bundle** view is displayed.

3. Enter a **Name** and a **Version** for the new task bundle.

   We recommend that you use the name "Android SSP task bundle" for task bundles that are applied during the enrollment process through the Self Service Portal.

4. Under **Operating systems**, select the compatible operating systems for the new task bundle. Select all Android settings for this task bundle.

   Note: The operating system list is created according to devices registered with the system. At this stage, it may show only **Android**. The setting **Android** covers all supported Android versions.

5. Click the **Create task** button.
6. As a first task, select **Enroll**. Enter a task name and click **Apply**. The name you define here is shown in the Self Service Portal while tasks are processed.
7. Create a second task of the type **Install profile**. Give the task a meaningful name, for example "Install provisioning profile", select the profile you have created ("Android SSP profile", if you have used the suggested name) and click **Apply**. If you have configured profiles with Exchange, VPN and Wi-Fi settings, repeat this step for each profile.
8. Repeat this procedure to add further tasks. You can set the order for installation for selected tasks by using the sort arrows on the right-hand side of the **Tasks** list.
9. After you have added all required tasks to the task bundle, click the **Save** button in the **Edit task bundle** view.

The task bundle is available for transfer. It is displayed in the **Task bundles** view. To create further task bundles, repeat the steps described.

16 Update Self Service Portal settings

After you have created the task bundles to be transferred when users register their devices with the Sophos Mobile Control Self Service Portal, you need to update the Self Service Portal settings with the required group settings:

1. In the web console menu bar, under **SYSTEM**, click **Setup** and then click **Self Service Portal**.

   The **Self Service Portal** view is displayed.

2. Go to the **Group settings** tab.
3. Under **Group settings**, click the blue triangle next to the **Default** Self Service Portal group and then click **Edit**.
4. From the **Enrollment package** drop-down list, select the task bundles you have created for iOS and Android devices.
5. Select the **Active** checkbox for the device types that should be available in the Self Service Portal:

   - **Android**
   - **iOS**

   Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, refer to the *Sophos Mobile Control administrator guide*.

6. From the **Add to device group** drop-down list, select the group that devices registered through the Self Service Portal should be added to.
7. Click **Apply**.
8. In the **Group settings** tab, click the **Save** button.

17 Create a Self Service Portal user with internal user management

Prerequisite:

- You selected **Internal directory** to use internal user management for users of the Sophos Mobile Control Self Service Portal when you created the customer.

To test provisioning through the Self Service Portal, create a Self Service Portal user account for yourself. With this user account you can log in to the Self Service Portal.

Note: The steps described refer to internal Self Service Portal user management. In this guide, internal Self Service Portal user management is described as an example. For information on external user management, see the *Sophos Mobile Control super administrator guide*.

1. In the web console, under **MANAGE**, click **Users**.

   The **Show users** view is displayed.

2. Click the **Create user** button.

   The **Edit user** view is displayed.

3. Enter the following information for the new Self Service Portal user:
   - **User name**
   - **First name**
   - **Last name**
   - **Email address**

The new Self Service Portal user is displayed in the **Show users** view. A welcome email is sent to the email address specified.

18 Test enrolling through the Self Service Portal

We recommend that you test provisioning through the Self Service Portal with one user before you roll out Self Service Portal use to further users.

Log in to the Self Service Portal with the Self Service Portal user account you have created for yourself and register and enroll devices. We recommend that you run a test for all platforms that you want to use with Sophos Mobile Control.

For further information on how to use the Self Service Portal, refer to the *Sophos Mobile Control user guide*.

Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, see the *Sophos Mobile Control administrator guide*.

19 Upload your user list to Sophos Mobile Control with internal user management

After you have tested enrolling through the Self Service Portal, you can import your user list to Sophos Mobile Control.

Note: The steps described here are only required for internal Self Service Portal user management. It is not necessary for external user management where all users assigned to a certain LDAP group, defined during LDAP configuration, can log in to the system. For information on external user management see the *Sophos Mobile Control super administrator guide*.

1. In the web console menu bar, click **Users**.

   The **Show users** view is displayed.

2. Click the **Import users** button.

   The **Import users** view is displayed.

   If you do not have a .csv file with users yet, you can download a sample file now and use it for creating your import file.

3. Make sure that the **Send welcome emails** checkbox is selected. The welcome email includes all required login credential information.
4. Click **Upload a file** and select the .csv file you want to import.

   The entries in the .csv file are checked for errors and displayed on the import page.

   Note: If there are any errors in the .csv file, it cannot be imported. An error message is displayed next to the relevant entries. Edit the .csv file accordingly and try again.

5. If all entries are correct, click the **Finish** button.

The users are imported and displayed in the **Show users** view. They can use the Self Service Portal for registering and enrolling their devices.

20 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

21 Legal notices